

09-22-00

A



Box Patent Application  
 ASSISTANT COMMISSIONER FOR PATENTS  
 Washington D.C., 20231

FORM PTO-1082  
 Case Docket No.: 81087-250501  
 Date: September 21, 2000  
 Express Mail Label No.: EL 594 171 844 US



Dear Sir:

Transmitted herewith for filing is the patent application of  
 Inventor(s): SHAUN ASTARABADI, GLENN SWONK, ANDREW MCCLOSKEY  
 For: SYSTEM OF DELIVERING CONTENT ON-LINE

Enclosed are:

- ☒ 9 Sheets(s) of informal drawings  
☒ An assignment of the invention to Toshiba America Information Systems, Inc.  
 \_\_\_\_\_ An associate power of attorney  
 \_\_\_\_\_ A verified statement to establish small entity status under 37 CFR1.9 and 1.27.  
☒ Declaration and Power of Attorney.  
 \_\_\_\_\_ Certified copy of Patent Application No. \_\_\_\_\_ filed \_\_\_\_\_ from which priority is  
 claimed under 35 U.S.C. §110.  
 \_\_\_\_\_ IDS enclosed. \_\_\_\_\_ with references.  
 \_\_\_\_\_ Preliminary Amendment.

CALCULATION OF FEES					
ITEM	NO. OF CLAIMS FILED MINUS BASE*	NO. OF CLAIMS OVER BASE	X SM/LG ENTITY FEE	\$ AMOUNT	FEE
A TOTAL CLAIMS FEE	28 -20*=	8	x \$9 or x \$18	\$ 144	
B INDEPENDENT CLAIMS FEE**	6 - 3*=	3	x\$39 or x 78	\$234	
C SUBTOTAL - ADDITIONAL CLAIMS FEE (ADD FINAL COLUMN IN LINES A + B)					\$378
D MULTIPLE-DEPENDENT CLAIMS FEE			SMALL ENTITY FEE = \$130 LARGE ENTITY FEE = \$250		\$
E BASIC FEE*			SMALL ENTITY FEE = \$345 LARGE ENTITY FEE = \$690		\$690
F TOTAL FILING FEE (ADD TOTALS FOR LINES C, D, AND E)					\$1068
G ASSIGNMENT RECORDING FEE					\$40
**LIST INDEPENDENT CLAIMS 1, 6, 11, 18, 25, 27					

\_\_\_\_\_ Please charge my Deposit Account No. \$ \_\_\_\_\_  
 \_\_\_\_\_ the amount of  
☒ A check in the amount of \$1068  
☒ A check in the amount of \$40

**A copy of this sheet is enclosed.**

to cover the filing fee is enclosed.

to cover Assignment Recordation fee is enclosed.

X The Commissioner is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to Deposit Account No. 03-3975. **A copy of this sheet is enclosed.**

X Any filing fees under 37 CFR 1.16 for the presentation of extra claims.

X Any patent application processing fees under 37 CFR 1.17.

\_\_\_\_\_ The Commissioner is hereby authorized to charge payment of the following fees during the pendency of this application or credit any overpayment to Deposit Account No. 03-3975.

\_\_\_\_\_ Any patent application processing fees under 37 CFR 1.17.

\_\_\_\_\_ The issue fee set in 37 CFR 1.18 at or before mailing of the Notice of Allowance, pursuant to 37 CFR 1.311(b).

\_\_\_\_\_ Any filing fees under 37 CFR 1.16 for presentation of extra claims.

Respectfully submitted,

Dated: September 21, 2000



Charanjit Brahma

Reg. No. 46,574

PILLSBURY MADISON & SUTRO LLP  
725 South Figueroa Street, Suite 1200  
Los Angeles, CA 90017-5443  
Telephone: (213) 488-7100  
Facsimile: (213) 629-1033

PATENT  
81087-250501

1c784 U.S. PTO  
09/666235



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

SHAUN ASTARABADI ET AL.

Serial No.: UNKNOWN

Filed: SEPTEMBER 21, 2000

Group No.: UNKNOWN

Examiner: UNKNOWN

For: SYSTEM OF DELIVERING CONTENT ON-LINE

CERTIFICATE OF MAILING VIA U.S. EXPRESS MAIL

"Express Mail" Mailing Label No. EL 594 171 844 US

Date of Deposit: September 21, 2000

Box NEW APPLICATION

Assistant Commissioner for Patents

Washington, D.C. 20231

Dear Sir:

I hereby certify that

- ☒ Letter of transmittal
- ☒ Check in the amount of \$1068 as filing fee.
- ☒ Patent application (19 pages of specification; 28 claims; 1 pages of abstract)
- ☒ 7 sheet(s) of informal drawings
- ☒ Declaration
- ☒ Executed assignment, with Recordation Cover Letter and check in amount of \$40
- ☒ Return postcard

are being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service with sufficient postage under 37 CFR 1.10 on the date indicated above and are addressed to:

Box NEW APPLICATION

Assistant Commissioner for Patents

Washington, D.C. 20231.

September 21, 2000

Date of Deposit

Gerald K. Pope

Name of person mailing papers

Signature

APPLICATION FOR  
UNITED STATES PATENT  
IN THE NAME OF

**Shaun Astarabadi**

**Glenn Swonk**  
and

**Andrew McCloskey**

Assigned to

**TOSHIBA AMERICA INFORMATION SYSTEMS, INC.**

for

**SYSTEM OF DELIVERING CONTENT ON-LINE**

prepared by:  
PILLSBURY MADISON & SUTRO LLP  
725 South Figueroa Street, Suite 1200  
Los Angeles, CA 90017-5443  
(213) 488-7100  
Attorney Docket No. 81087-250501

Express Mail No.: EL 594 171 844 US

# SYSTEM FOR DELIVERING CONTENT ON-LINE

This is a Continuation-in-part of U.S. Patent Appl. Ser. No. 09/553,430 filed on April 19, 2000.

5

## BACKGROUND

### 1. Field of the Invention:

Embodiments described herein relate to services to provide media content. In particular, 10 embodiments herein relate to providing media content in computer networks.

### 2. Related Art:

Traditional methods of distributing media content such as movies or music have involved the sale or rental of portable media such as video cassettes, compact disks or magnetic tapes, etc. The evolution of data communication networks has expanded the possibilities by which media 15 content may be delivered to consumers. This has reduced the need for the expensive procedure associated with of the distribution of portable media associated with maintaining retail facilities and an inventory of media content titles.

The use of data communication networks also allows the distribution of digitized content in standard formats (e.g., MPEG2 for video content) which permits a presentation of the content 20 on customer equipment with minimal signal noise corrupting the presentation on the customer equipment. Unfortunately, once digitized content is delivered to the customer over a data communication network, the customer is typically able to copy and distribute the content using commonly available technology without authorization from the owner of the content.

Accordingly, there is a need for systems and techniques to prevent and discourage customers 25 from copying and distributing content delivered in a data communication network.

## BRIEF DESCRIPTION OF THE FIGURES

Figure 1 shows a network topology including a local server according to an embodiment.

Figure 2 shows a schematic diagram illustrating the hardware architecture of the local server of Figure 1 according to an embodiment.

5        Figures 3A, 3B and 3C show a functional flow diagram of a process for establishing a communication protocol between the local server of Figure 1 and one or more client computer workstations in a private network according to an embodiment.

Figure 4 shows a diagram illustrating a process of transmitting print jobs from a client computer workstation to a parallel port printer through a print queue at an embodiment of the local server shown in Figure 2.

Figure 5 shows a flow diagram illustrating a process of combining digitized content with an encoded signal identifying a subscribing party according to an embodiment.

Figure 6 shows a flow diagram illustrating an embodiment of the process of Figure 5 in which identification data is inserted into video frames of digitized content.

Figure 7 shows a home page for a turnkey Intranet according to an embodiment of the present invention.

## DETAILED DESCRIPTION

Embodiments of the present invention are directed to providing media content to subscribers in an on-line environment. A remote server may provide digitized media content to a subscriber's local server through a digital communication network for storage at a local memory.

5 The local server is configured to stream the media content data to users at client devices. In one embodiment, the client devices may access the locally stored media content only through an agent process. In another embodiment, the remote server combines the digitized content with encoded data identifying the subscriber.

Figure 1 shows a network topology including a local server 2 coupled to client computer workstations 20 through links 8 and an integrated hub 4. In the illustrated embodiment, the integrated hub provides a plurality of Ethernet connections 6, each Ethernet connection 6 being adapted to be coupled to a distinct computer workstation 20 through a corresponding data link 8.

The local server 2 also includes a parallel port 10 coupled to a parallel port printer 12 and an Ethernet port 16. The Ethernet port 16 may be coupled to a broadband data source 26 such as a cable service or digital subscriber line (DSL) service through a compatible broadband modem 14. Alternatively, the port 16 may be coupled to other broadband data sources such as broadband satellite or terrestrial wireless communication services. In yet another embodiment, the port 16 is coupled to a local area network (LAN) or wide area network (WAN) as part of a larger private network.

20 The local server 2 may implement a firewall for monitoring data traffic between the data source 26 and the client computer workstations 20. In the embodiment in which the local server 2 is part of a larger private network such as a LAN or WAN, such a firewall may be provided at

a gateway which transports data between a public data communication network and the private network.

In the illustrated embodiment, a remote server 18 may communicate with the local server 2 through a public data communication network such as the Internet 22. Also, the local server 2 includes a dial-up modem 24 to enable point to point communication with a remote mobile client user.

Each of the client computer workstations 20 may have a keyboard, display, and pointer device such as a mouse or track ball. The client computer workstation may also host an operating system which supports a graphical user interface (GUI) such as Windows 98, Windows 2000 or Windows NT 4.0 sold by Microsoft. Accordingly, the client computer workstations 20 include sufficient CPU and random access memory (RAM) resources to support the hosted operating system. Additionally, the computer workstations 20 may include a network card and corresponding Ethernet port for communicating with the local server 2 through the links 8. The client computer workstations 20 may also include a memory drive for receiving a removable memory medium such as a CD ROM drive or floppy disk drive in addition to a hard drive with a fixed memory. The communication link 8 coupling the client computer workstations 20 to the hub 4 may be an Ethernet cable or a wireless link coupling the Ethernet port of the client computer workstation 20 to a corresponding Ethernet port 6 on the hub 4. Such a wireless link may be compliant with the Bluetooth protocol or other known wireless communications format suitable for supporting bi-directional communication in a local environment.

Figure 2 shows a schematic diagram illustrating the architecture of 50 of the local server 2 according to an embodiment. A central bus 68 is coupled to a CPU 52, RAM 54, and hard disk drive (HDD) 56. The CPU 52 may be a 200 megahertz Celeron processor sold by Intel or other



compatible microprocessors sold by other manufacturers such as Advanced Micro Devices (AMD). The architecture 50 may host a version of the Linux operating system or other suitable operating system which supports a communication protocol between the local server 2 and the client computer workstations 20, and between the local server 2 and the data source 16 (Figure 1). Such communication protocols may include, for example, TCP/IP and the hypertext transfer protocol (HTTP). The architecture 50 also includes several communication devices coupled to the bus 68 including an Ethernet card 58 (for enabling communication with the Ethernet port 16), a parallel port controller 60 (for enabling communication with the printer 12 through the parallel port 10), an Ethernet card 62 (for communication between the hub 4 and the client computer workstations 20), a universal asynchronous receiver/transmitter (UART) 64 (enabling point to point communication through the modem 24). The architecture 50 may be provided in a chassis within a single form factor enclosure as shown in the local server 2 of Figure 1. The hub 4 may allocate network addresses to the client computer workstations 20 according to a dynamic host control protocol (DHCP) or may allocate such network addresses statically. The Ethernet port 16 may be assigned a network address from the data source 16 either statically or according to the DHCP.

The architecture 50 may include a control panel 70 which is external to the chassis enclosure of the local server 2 to be accessible by an operator or system administrator. The control panel 70 may include, among other things, an LCD display and selection buttons (not shown) which enable the operating system administrator to request specific status information be displayed on the LCD display. A controller 66 enables communication from the selection buttons to the processing hardware and from the processing hardware to the LCD display for showing the requested status information.

According to an embodiment of the present invention, a removable computer readable medium such as a CD ROM or floppy disk is inserted into a removable medium drive of the client computer workstations 20 to establish a communication protocol between the client computer workstation 20 and the local server 2. Figures 3A through 3C illustrate a process of  
5 executing a procedure stored on the computer readable medium to establish communication between a client computer workstation 20 and the server 2 according to an embodiment. Step 102 determines a particular operating system residing on the client computer workstation 20. For example, the operating system may be any one of several versions of Microsoft windows such as Windows 98, Windows 2000 and Windows NT 4.0. The operating system may be a  
10 version of any one of several other operating systems which support a GUI on the client computer workstations such as versions of the Macintosh operating system sold by Apple Computer or OS2 sold by IBM. Also, the operating system may also be versions of Linux or DOS.

Based upon knowledge of the particular operating system version, step 104 can determine whether network communication enabling software, such as software drivers for an Ethernet card, have been installed on the hard drive of the client computer workstation 20. If the network software is not installed, step 106 provides a message to the user instructing installation of the network software by, for example, instructing the user to install the network software from the operating system CD provided by the operating system manufacturer. Step 110 waits for a  
15 response from the user indicating that such network software has been installed, and step 104 is repeated to determine whether the network software has been installed.

Following the determination that the network software has been installed, step 108 determines whether an Ethernet controller card has been installed. This is accomplished by, for

example, polling the software drivers for the Ethernet controller. If no Ethernet controller is detected, step 112 provides a message to the user that no Ethernet controller has been installed. If an Ethernet controller is installed, step 114 sets network parameters in the network software driver stack to enable TCP/IP communications through the Ethernet port. Step 116 then “pings” the hub 4 at the local server 2 with a known IP address. In the illustrated embodiment, the local server 2 is assigned a known IP address such as “192.168.1.1” which is indicated in the program for configuring the client computer workstation 20 for communication with the local server 2 on the removable medium. If the client computer workstation 20 does not receive a response from the local server 2 at step 118, step 120 displays a message to the user to check the physical connection between the Ethernet port of the client computer workstation 20 and the hub 4, and check the IP address of the local server 2. In the illustrated embodiment, the address of the local server 2 may be changed by a remote administrator via an agent as discussed below, or by physical tampering with the local server 2. The control panel 70 (Figure 2) may receive input selections from a user having physical access to the local server 2 for requesting display of the assigned network address of the local server 2 on the LCD display of the control panel 70. This may be accomplished by, for example, associating a particular interrupt routine responding to signals from the controller 66 to retrieve the network address of the local server 2 from memory and display on the LCD display. Accordingly, the user may compare the network address provided on the LCD display with the network address displayed at the client computer workstation 20 and input the correct network address of the local server 2 if there is no match. Step 122 waits for a user to respond to the message at step 120 to attempt to ping the server again at step 116.

Upon receipt of a response to the ping from a local server 2, step 124 executes a script at the local server 2 to establish communication at the HTTP layer. Execution of the script results in transmission of information identifying the local server and administrative status which is received by the client computer workstation 20 at step 126. This information may include, among other things, the manufacturer of the local server 2, model number, version number, and version of the operating system at the local server 2. This information received at step 126 may also include administrator status information indicating whether a client user has been designated as the network administrator, and any pre-authorized client users.

If step 128 determines that an administrator has been designated, step 130 initiates an authentication process for the user by displaying a query at the client computer workstation 20 for a user name. If the user inputs a user name included in a list of pre-allocated user names received at step 126, step 134 initializes a process to establish a user's password by, for example, asking the user to select a password of appropriate character length.

If step 128 determines that a network administrator has not been designated, step 132 displays a prompt to the user asking the user if the user would like to be the designated administrator. If the user does not accept, the process terminates at step 138. Alternatively, if the user accepts, step 140 prompts the user to create a user name and password for the administrator and step 142 prompts the user to establish user names for other users for future use (e.g., at steps 130 and 134 for authenticating non-administrative users and their passwords).

In the illustrated embodiment, the designated administrator has certain privileges to the exclusion of other client users of the local server 2. For example, the designated administrator may have privileges to add or delete user accounts, retrieve password information for other client users and allocate memory resources on the HDD 56 (Figure 2). The manufacturer of the local

server 2 may maintain a remote server 18 shown in Figure 1, which may communicate with the local server 2 through the Internet 22. Data source 26 may allocate a worldwide web address to the Ethernet port 16. According to an embodiment, the designated administrator has the ability to delegate or handoff administrative privileges to a remote server 18 through the Internet. This  
5 may be implemented in the form of an agent process residing at the local server 2 which is controlled by the administrator at the remote server 18 upon assuming administrative privileges. The handoff of administrative privileges may be invoked by a message received from the local administrator through the public data communications network or by a telephone call. The administrator at the remote server 18 may have additional privileges for access to operating system or system configuration files to diagnosis malfunction and take appropriate corrective  
10 action.

The HDD 56 may be used to store centralized files for a small business or enterprise which is essential to the functioning of the small business or enterprise. It, therefore, may be desirable to periodically backup the files of the HDD 56 to another memory device such as a backup tape drive or CD ROM press (not shown) coupled to the local server 2. In an alternative  
15 embodiment, the backup device may be attached to one of the client computer workstations 20 or at a remote location. An embodiment of the present invention is directed to receiving an input at the control panel 70 (e.g., a predetermined or menu driven selection of buttons or keystrokes) to initiate a backup of the entire image, or portions thereof, stored on the HDD 56. For example,  
20 input interpreted at the controller 66 may initiate or interrupt to execute a routine at CPU 52 to copy files from HDD 56 to the aforementioned backup memory device coupled to the local server 2. In an alternative embodiment, the backup routine may include transmitting the files to be backed up from the HDD 56 to the remote server 18 via the Internet 22. The remote server 18

may provide such a service to the operator or local server 2 on a subscription basis. The remote server 18 may then maintain backup files for the operator or local server 2 which are available upon request.

Another embodiment of the present invention is directed to implementing a print server for the printer 12 at the local server 2 which enables the client computer workstations 20 to share the printer 12 (Figure 1). Figure 4 illustrates an implementation of such a system which enables sharing of the printer 12. Here, the user creates a document for printing at an application 202 and request that the document be printed. A printer driver 204 creates a print job from the document received from the application 202. The print job created at the printer driver provides printer commands and image data in a suitable form to be received at the printer 12. For example, the created print job may include image data and printer commands interpretable by the printer 12 to accurately reproduce the document created at the application 202. The print job may be a form suitable for transmitting to a low level parallel port driver associated with a port coupled to a parallel port printer. In the illustrated embodiment, the print job is packetized and provided to a transport protocol driver 208 to be transmitted to the local server 2 through an Ethernet port 210 and communication link 8.

The packetized print job is received at the hub/Ethernet port 4 and provided to a print server 214 via an IP server 212. Print jobs received from the IP server 212 are depacketized and reassembled at a depacketize routine 216. The reassembled print jobs are suitable for transmitting to the printer 12 through a low-level parallel port driver. A print queue 218 stores and sequentially releases print jobs to the parallel port printer 12 through the low level parallel port driver 220 and parallel port 10. In an alternative embodiment, the print jobs may be depacketized as they are released from the print queue 218.

The print server 214 at the local server 2 enables the local server 2 to be used with any parallel port printer without having the software driver of the parallel port printer. Accordingly, no modifications are required to the local server 2 when a new parallel port printer (i.e., having a different print job format) is used. The client computer workstations 20 include the printer driver 204 which is compatible with the particular parallel port printer 12 coupled to the parallel port 10. Therefore, when a different parallel port printer 12 is coupled to the parallel port 10, a printer driver 204 which is compatible with the new printer may be enabled or installed at the client computer workstations 20.

Another embodiment of the present invention is directed to displaying information regarding the status of the local server 2 on the display portion of the client computer workstation 20. The operating system on a client computer workstation 20 may have logic for generating a particular image in the display in response to an absence of processing activity at the CPU of the client computer workstation 20. For example, versions of the Windows Operating System include logic for a "screen saver" which generates an image to be displayed after a prolonged period of an idle state at the CPU. In the illustrated embodiment, such screen saver logic may include a routine for transmitting a polling signal to the local server 2 for status information including, for example, the number of users currently actively logged into the system, available memory on the HDD 56, date of the last system backup, CPU utilization, and other such status information. Thus, the screen saver routine periodically transmits a polling signal down the network stack to be transmitted through the communication link 8 and received at the IP server of the local server 2. A status routine at the local server 2 responds to the polling signal by retrieving the status information from designated memory locations in the RAM 54 and transmitting information which is representative of the retrieved status information back to the

requesting client computer workstation 20. The screen saver routine at the client computer workstation 20 interprets the received information and generates an alphanumeric display on the display screen to show the status information to the user.

According to an embodiment, the controller 66 associated with the control panel 70 may include logic for performing power up and power down procedures for the local server 2 according to a pre-specified schedule (Figure 2). According to an embodiment, the CPU 52 resides on a motherboard. Here, the controller 66 maintains an internal clock and receives power from a power supply (not shown) in the local server 2 independently of the power source to the motherboard, RAM 54 and HDD 56. Logic in the controller 66 allows a system operator to specify a schedule for powering up and powering down the local server 2 (e.g., by specifying a time and date when the local server 2 is to be powered down and a time and date when the local server 2 is to be powered up).

To initiate a procedure to power down the local server 2, the controller 66 may transmit an interrupt signal to initiate the execution of a driver for shutting down the operating system. The controller 66 may then monitor the progress of the shut down procedure to detect completion by, for example, detecting a signal from the driver indicating completion of the shut down procedure or detecting an absence of a signal from the driver indicating that the shut down procedure is still in progress.

Upon determining that the shut down procedure has completed, the controller 66 may transmit a signal to the power supply to remove power from other select devices of the local server 2 such as the motherboard, the RAM 54 and the HDD 56. In an embodiment in which the power supply is digitally controlled, the controller 66 may transmit a power down signal to the power supply on a bus (not shown) to remove power from the select devices. Alternatively, the



controller 66 may transmit a signal to a relay switch which causes the removal of power to the select devices. To restore power to the select devices of the local server 2, the controller 66 transmits a signal to the power supply to restore power to the select devices. Upon receipt of power at the motherboard, the local server 2 may re-boot or return to a state at which the local server 2 was previously shut down.

Other embodiments of the present invention are directed to serving content to the client computer workstations 20 from the remote server 18. For example, a user at a client computer workstation 20 may request that the remote server 18 provide contents such as video and/or audio content to be stored at the HDD 56 in digital form, and then streamed to any client computer workstation 20 on demand for presentation on demand.

In one embodiment, an agent process (not shown) of the remote server 18 resides on the local server 2. A request from the user at the client computer workstation for content at the remote server 18 initiates the agent process. The agent process receives the digitized content from the remote server 18 and installs the digitized contents on the HDD 56. As part of a subscription agreement, the digitized content may be available for presentation to any one of the client computer workstations 20 for a specified subscription period. When the user requests presentation of the content at a client computer workstation 20, the agent process responds by retrieving the digitized content from the HDD 56 and streaming the content to the client computer workstation 20 for the display of the content on the display on the client computer workstation 20 (in the case of video content) or playing the content through speakers (not shown) at the client computer workstation 20 (in the case of audio content).

According to an embodiment, the operating system on the local server 2 partitions the HDD 56 such that at least one dedicated portion of the HDD 56 is accessible by the agent

process and is not accessible by any of the users at the client computer workstation 20. This prevents the users from accessing the dedicated portion of the HDD 56 for the purpose of copying the digitized content in violation of the subscription agreement. In another embodiment, the agent process removes the digitized content from the dedicated partition upon expiration of the subscription period. This prevents users from presenting the content at the client computer workstations 20 beyond the subscription period.

According to an embodiment, the remote server 18 provides requested digitized content to the agent process having encoded information identifying the subscriber. The digitized content which is then stored on the HDD 56 in the dedicated partition includes encoded information identifying the subscriber. Therefore, to the extent that a subscriber may copy and/or distribute the delivered content without authorization, the distributed copies will retain the encoded information identifying the subscriber.

Figure 5 illustrates a process by which the remote server 18 provides digitized content to the agent process at the local sever 2 in response to a user request. At step 302, the remote server 18 receives a request for a particular content title from the agent process. In addition to identifying the particular requested title, the request also includes information from which the identity of the subscriber may be obtained. For example, the request may include information identifying the particular local server 2 which is cross-referenced with the subscriber's identity. The request may also specifically identify the subscriber by a subscriber's name or by an account number.

At step 304 the remote server 18 retrieves encoded digital data identifying the subscriber. At step 306 the remote server 18 retrieves the digitized content title from a content server as

identified in the received request. Step 308 combines the encoded identification data retrieved at step 304 with the digitized content title retrieved at step 306 to provide modified digitized content. The combined data is then compressed and transmitted back to the agent process at step 310 to be stored on the HDD 56. The digitized content stored on the HDD 56, therefore,  
5 includes the encoded data identifying the subscriber.

Figure 6 illustrates an embodiment of processing of steps 304, 306 and 308 for a digitized content title in a video format. In the illustrated embodiment, a “watermark” is inserted into the video frames which are displayed to the users when streamed to the client computer workstation 20 for presentation. The watermark may include, among other things, the name of the  
10 subscriber, an account number or an icon identifying the subscriber. Step 402 receives video content in an analog format such as VHS. In an alternative embodiment, the video content may be stored in a digital compressed format such as MPEG 2. In the embodiment in which video content is received in an analog format, step 404 digitally captures the video frames to provide an “.avi” file for the video frames. In the embodiment in which video titles are retrieved in a  
15 compressed digital format, step 404 decompresses the data to extract the digitized video frames. Step 406 inserts the watermark into the digitized video frames to provide a combined video signal using video editing techniques known to those of ordinary skill in the art. Step 408 then compresses the combined video signal into a compressed format such as MPEG 2 for transmission to the agent at the local server 2.

20 While the embodiments illustrated above are directed to inserting encoded information into the digitized content which to be then stored in the dedicated partition of HDD 56, it should be understood that the embodiments illustrated above with reference to Figures 5 and 6 may be applied to digital content delivery systems generally. For example, systems for providing video

on demand to subscribers through a cable television set top box may also employ the illustrated technique for inserting a watermark. Here, a cable television head-end may receive a request for a video title from a subscriber. Based upon the identity of the subscriber, the head-end inserts a watermark into the video frames transmitted to the subscriber. In an embodiment which the video on demand system transmits digitally encoded audio and video data, the head-end transmits the video data after the watermark is inserted and any following digital compression and packetization. In an embodiment which the head-end provides the video on demand in an analog rasterized video signal, the head-end generates an analog video signal based upon the digitized video frames including the combined digital watermark. The modified digitized video frames may then be converted back to an analog rasterized video signal for transmission to the subscriber.

The insertion of encoded data identifying a subscriber may also be used in content delivered on removable memory devices such as video tapes, compact disks, and other removable media capable of storing a content title in a digital or analog format. For example, a subscriber may order a content title which is to be prepared on the removable medium. The content title is first provided in a digital format, and then combined with the encoded data representative of the identity of the customer. Such an insertion of the encoded data identifying the customer may discourage the customer from unauthorized copying and distribution of the content.

In one embodiment of the present invention, the local server may include a factory loaded turnkey Intranet which is accessible at network browsers at the client workstations 20. Figure 7 shows a home page 500 for an embodiment of the turnkey Intranet which may appear at a client computer workstation 20 when an instance of the network browser is launched at the client

computer workstation 20. The home page 500 may be generated from an HTML document and includes fields 520, 522, 524, 526 and 528. Fields 520, 522, 524, 526 and 528 may be provided as blank fields to be custom tailored according to the functions of an organization using the local server 2. Authority to modify these fields may be restricted to certain users such as the system administrator.

The home page 500 also includes selectable icons 502 through 514. Each of the selectable icons 502 through 514 is associated with a script which is executed upon selection of the icon. The scripts for the icons 502, 510, 512 and 514 may link the network browser to HTML pages hosted at the local server 2 which are maintained by the enterprise. Each of these local HTML pages may be maintained by one or more designated users to provide internal information resources to the users. Selection of the icon 510 may provide a page which allows the downloading of one or more internal documents or forms. Selection of icons 512 or 514 may provide pages containing information which is updated internally on a periodic basis.

Each script for the icons 504 through 508 provides a link to a universal resource locator (URL) of a server process hosted at or in conjunction with the remote server 18. These scripts may request a page from the remote server 18. The operator of the remote server 18 may update the pages associated with the icons periodically to ensure that the information and links at each URL is current. Selection of the icon 504 may execute a script to request a page from the remote server 18 with links to one or more websites of third party vendors. The remote server 18 may host web based software applications for use by client users at the client computer workstations 20 for a fee. Selection of the icon 508 may execute a script to link the network browser to a server hosted at the remote server 18 to provide the web based applications. The remote server

18 may respond by, for example, providing pages with a menu of selectable options and a form for account authentication.

Selection of the icon 506 links the network browser to processes at the remote server 18 for dispensing digitized content as illustrated above with reference to Figures 5 and 6. The remote server 18 may provide a page with a form for receiving inputs from the network browser for account authentication and receiving content title selections. The remote server 18 may then dispense the selected content title via the agent process hosted on the local server 2 as discussed above.

The remote server 18 may operated by a provider of data services to a subscriber enterprise where the service provider furnishes or installs the local server 2 at a premises of the subscriber enterprise. The service provider may provide the local server 2 with computer instructions pre-loaded onto the HDD 56 for providing the Intranet system including instructions for generating the home page 500 at the GUI screens of the client computer workstations 20. Upon installation of the local server 2 at the premises of the subscriber enterprise, a user may order data services from the remote server 18 through a network browser by selecting an icon in the home page 500.

While there has been illustrated and described what are presently considered to be the preferred embodiments of the present invention, it will be understood by those skilled in the art that various other modifications may be made, and equivalents may be substituted, without departing from the true scope of the invention. Additionally, many modifications may be made to adapt a particular situation to the teachings of the present invention without departing from the central inventive concept described herein. Therefore, it is intended that the present invention

not be limited to the particular embodiments disclosed, but that the invention include all embodiments falling within the scope of the appended claims.

## CLAIMS

What is claimed is:

1. A method of providing media content to a subscriber, the method comprising:  
5 receiving a request for the transmission of the digitized content from the subscriber;  
retrieving the requested content from a content source;  
combining the requested content with encoded information identifying the requesting  
subscriber to provide modified content; and  
transmitting the modified content to the subscriber,  
10 wherein the encoded information in the modified content identifies the subscriber.
2. The method of claim 1, the method further comprising:  
providing a digitized image of the requested content including digitized video frames;  
and  
15 inserting a digitized image identifying the subscriber into at least some of the digitized  
video frames to provide the modified content.
3. The method of claim 2, the method further comprising:  
retrieving the requested content from a medium in an analog video format; and  
20 digitizing the retrieved content to provide the digitized image.
4. The method of claim 2, the method further comprising retrieving the digitized image  
from a digital storage medium.



5. The method of claim 2, the method further comprising:

converting the modified content from a digital format to an analog video format to provide analog content; and  
transmitting the analog content to the subscriber.

5

6. A server for providing media content to a subscriber, the server comprising:

a communication port for receiving transmissions from a client process associated with the subscriber, the received transmissions including a request for the transmission of the content;  
circuitry for retrieving the requested content from a storage medium;

logic for associating the received request with encoded information identifying the subscriber;

logic for combining the retrieved content with the encoded information to provide modified content; and

a communication port for transmitting the modified content to the subscriber,  
wherein the encoded information in the modified content to identify the subscriber.

7. The server of claim 6, wherein the media content includes a digitized image of the requested content including digitized video frames and the server further includes circuitry for inserting a digitized image identifying the subscriber into at least some of the digitized video frames to provide the modified content.

8. The server of claim 7, the server further comprising:

circuitry for retrieving the requested content from a medium in an analog video format;

and

circuitry for digitizing the retrieved content to provide the digitized video frames.

- 5 9. The server of claim 7, the server further comprising circuitry for retrieving the digitized image from a digital storage medium.

10. The server of claim 7, the method further comprising:

circuitry for converting the modified content from a digital format to an analog video

10 format to provide analog content; and

circuitry for transmitting the analog content to the subscriber through an analog video transmission medium.

11. A system for providing digitized media content to one or more subscribers, the system comprising:

a client process associated with each subscriber for receiving subscriber inputs and presenting the digitized content to the subscriber;

a client processor having a memory for storing digitized content for presentation to the subscriber;

- 20 a server for transmitting selected digitized content to the client processor for storage in a portion of the memory; and

an agent process associated with the server and hosted on the client processor for retrieval of the digitized content for presentation through the client process in response to requests of the client process,

wherein the client process is prevented from accessing the portion of memory  
5 independently of the agent process.

12. The system of claim 11, wherein the digitized content stored in the portion of the memory is available for presentation to the subscriber for a subscription interval and is not available for presentation to the subscriber after the subscription interval.

10 13. The system of claim 12, wherein the agent process removes the digitized content from the portion of memory when the subscription interval expires.

14. The system of claim 11, wherein the client process is hosted on the client  
15 processor.

15. The system of claim 11, wherein the client process is hosted on a client device which is distinct from the client processor, and wherein the client processor hosts a local server for providing content to the client process through a data network.

20 16. The system of claim 11, wherein the server provides the digitized content to the client processor through a data communication network including at a least a portion of a public data communication network.

17. The system of claim 16, wherein the public data communication network includes the Internet.

5 18. A method of providing media content to one or more subscribers, the method comprising:

transmitting digitized content from a server to an agent process hosted on a client processor including a memory for storing data;

10 executing the agent process for storing the transmitted media content in a portion of the memory;

executing the agent process for retrieving the stored media content for presentation at one or more client processes associated with the one or more subscribers; and

15 inhibiting the client processes from accessing the portion of memory independently of the agent process.

19. The method claim 18, the method further comprising:

presenting the digitized content stored in the portion of the memory at the one or more client processes under control of the agent process upon request from the one or more client processes during a subscription interval; and

20 inhibiting presentation of the digitized content upon expiration of the subscription interval.

20. The method of claim 19, the method further comprising removing the digitized content from the portion of the memory upon expiration of the subscription interval.

21. The method of claim 18, the method further comprising hosting the client process  
5 on the client processor.

22. The method of claim 18, the method further comprising:

hosting the client process a client device which is distinct from the client processor; and

10 hosting a local server on the client processor for providing content to the client processor through a data network.

23. The method of claim 18, the method further comprising transmitting the digitized content from the server to the client processor through a data communication network including  
15 at a least a portion of a public data communication network.

24. The method of claim 23, wherein the public data communication network includes the Internet.

20 25. A system for providing digitized media content to one or more subscribers, the system comprising:

a client process associated with each subscriber for receiving subscriber inputs and presenting the digitized content to the subscriber;

a client processor having a memory for storing digitized content for presentation to the subscriber;

a server for transmitting selected digitized content to the client processor for storage in a portion of the memory; and

5 an agent process associated with the server and hosted on the client processor for retrieval of the digitized content for presentation through the client process in response to requests of the client process for a subscription interval,

wherein the agent inhibits presentation of the digitized media content to the client process upon termination of the subscription interval.

10 26. The system of claim 25, wherein the agent process removes the stored digitized content from the memory upon termination of the subscription interval.

15 27. A method of providing on-line services from a service provider to a subscribing enterprise, the method comprising:

encoding on a non-volatile memory of a server appliance computer readable instructions for establishing an Intranet to enable communication among devices associated with the subscribing enterprise and for generating one or more enterprise pages for display in graphical user interfaces at the devices, at least one of the enterprise pages having selectable icons;

20 installing the server appliance at a premises of the subscribing enterprise; and

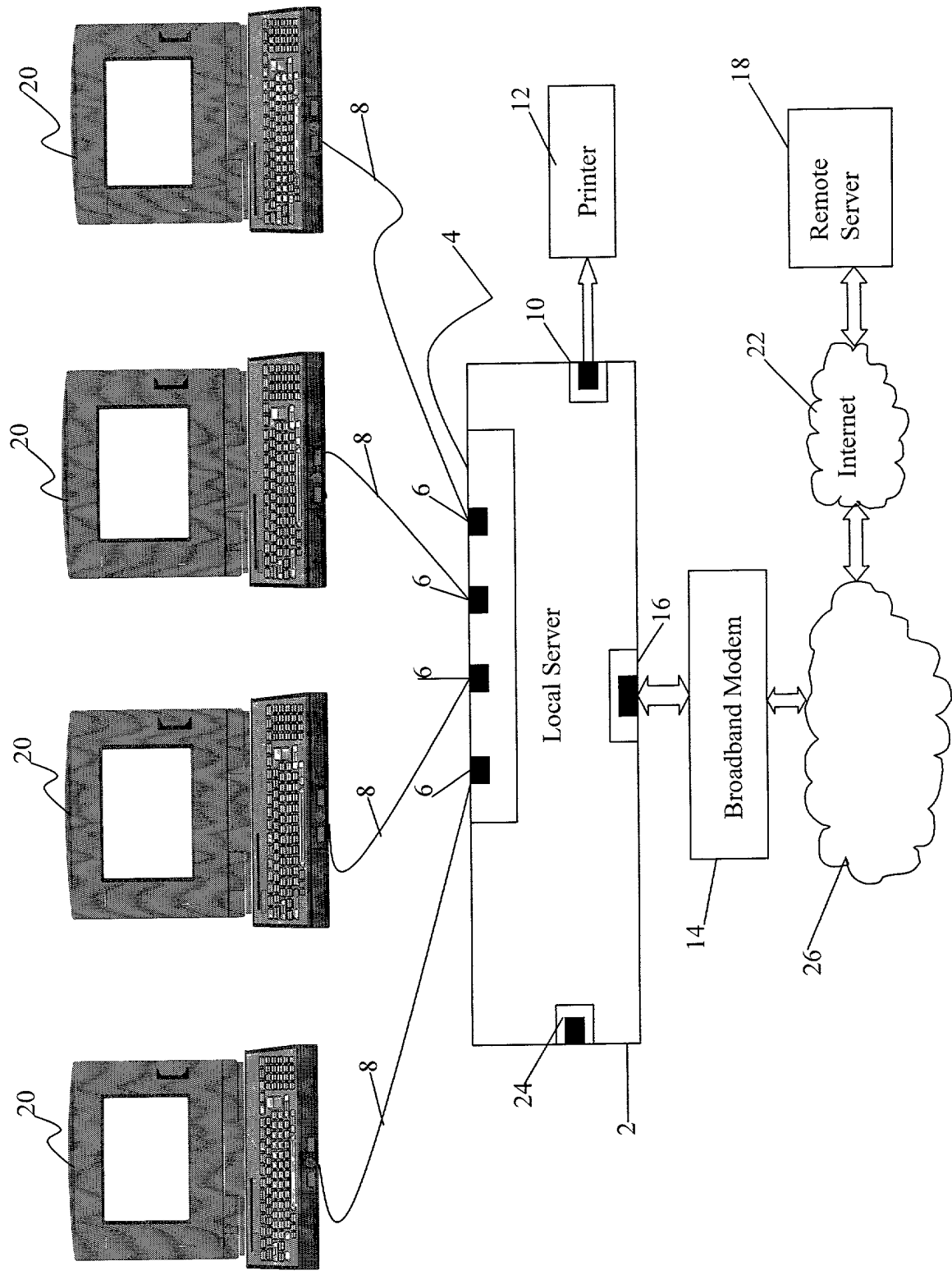
in response to selection of at least one of the icons at a graphical user interface, establishing communication between the server appliance and a server of the service provider through a public data communication network to provide a data service.

28. The method of claim 27, the method further comprising in response to the selection of the icon, transmitting data from the server of the service provider to the server appliance including a menu for the selection of services.

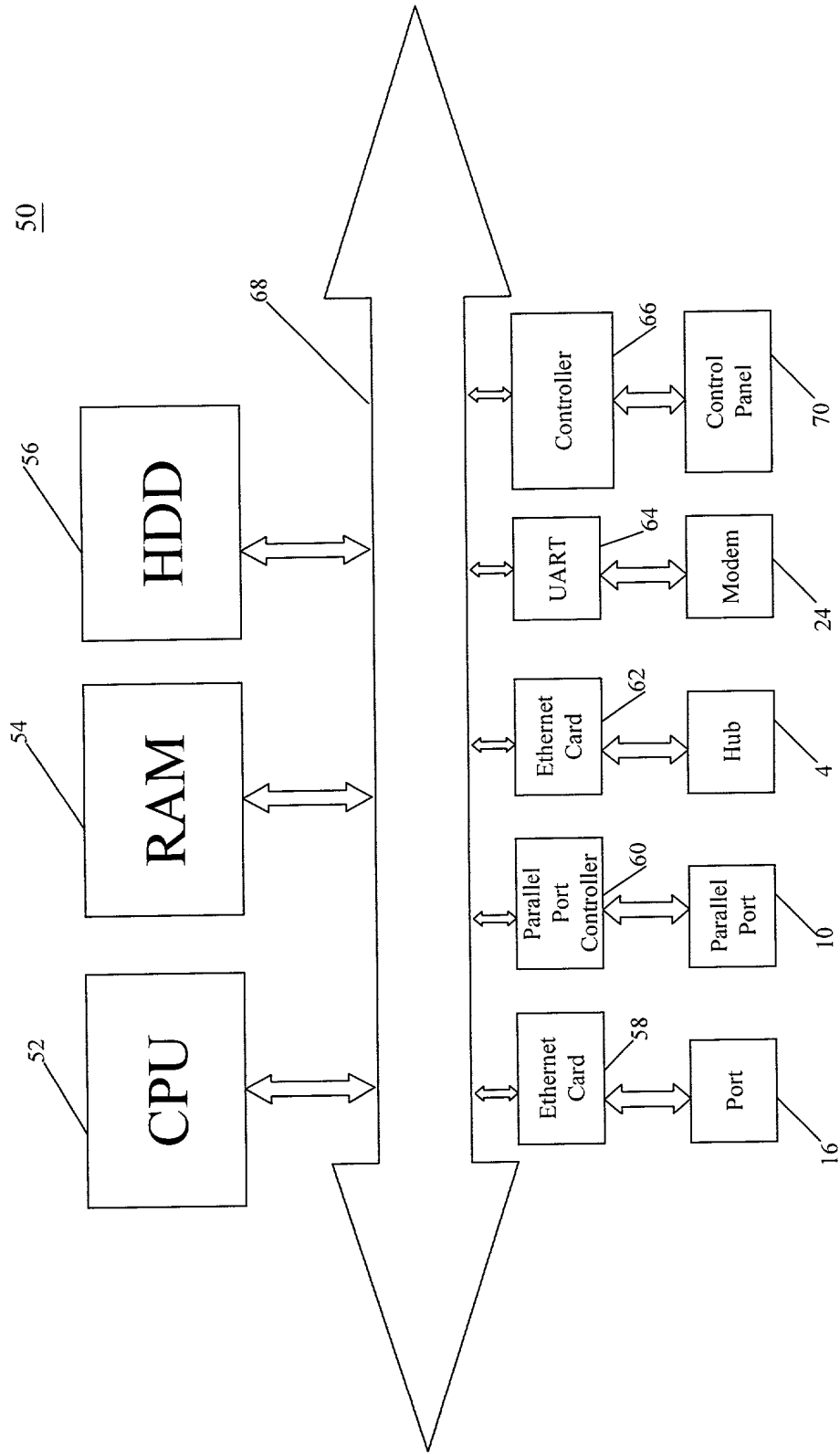
## ABSTRACT

A system and method of providing digitized media content from a remote server through a data network is disclosed. A local content server at the premises of the subscriber hosts an agent process and includes a memory for storing the digitized content. The digitized content  
5 may be streamed on demand to client devices through the agent process for a subscription period. However, the subscriber is prevented from otherwise accessing the digitized content from the local server. Also, the digitized content delivered from the remote server to the local server is combined with encoded data identifying the subscriber.

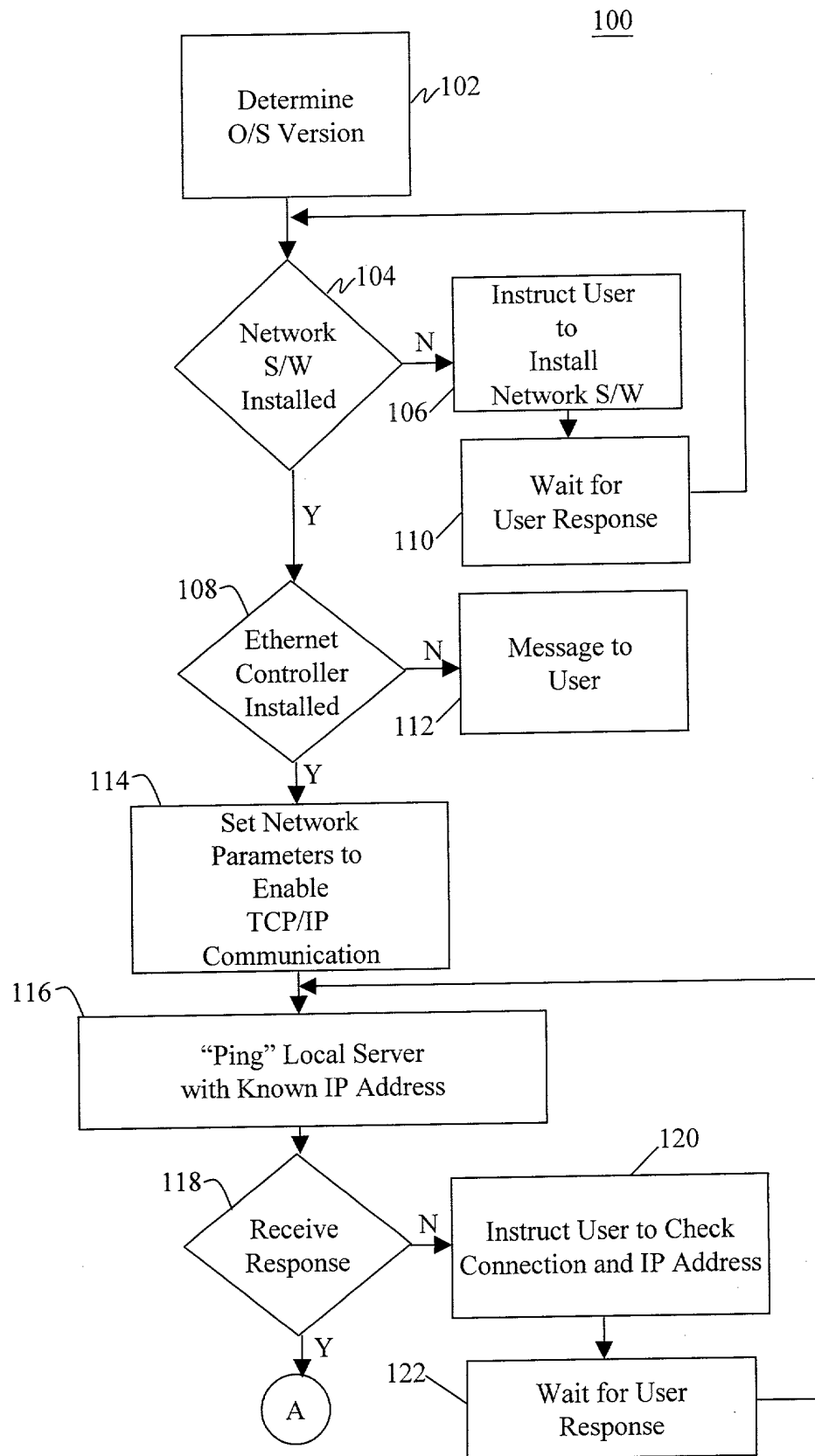




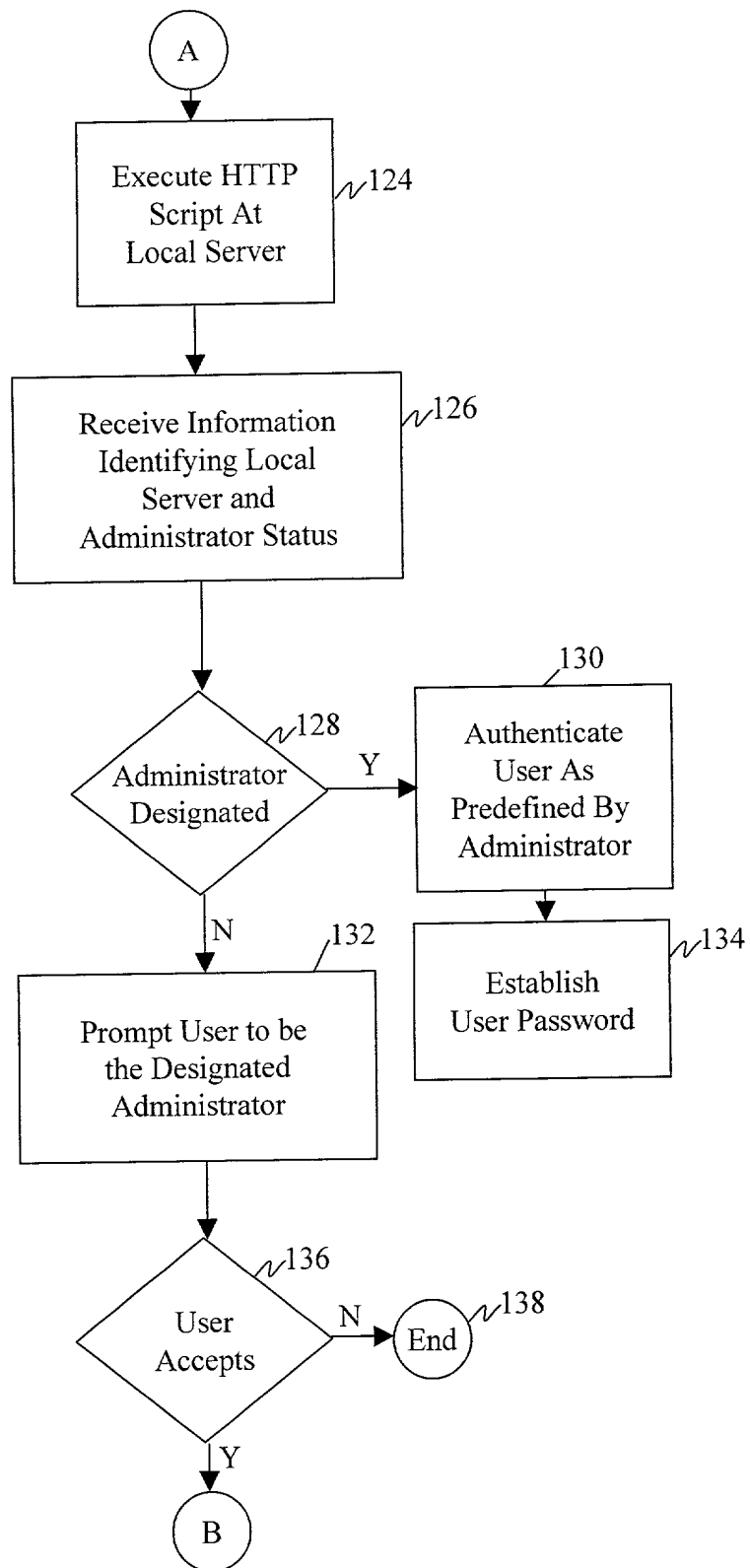
**Figure 1**



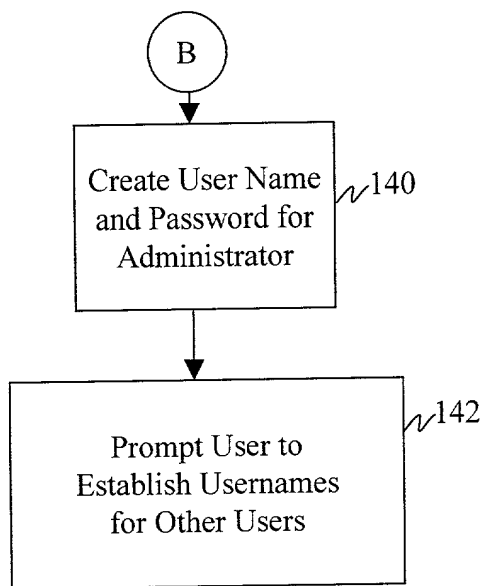
**Figure 2**



**Figure 3A**

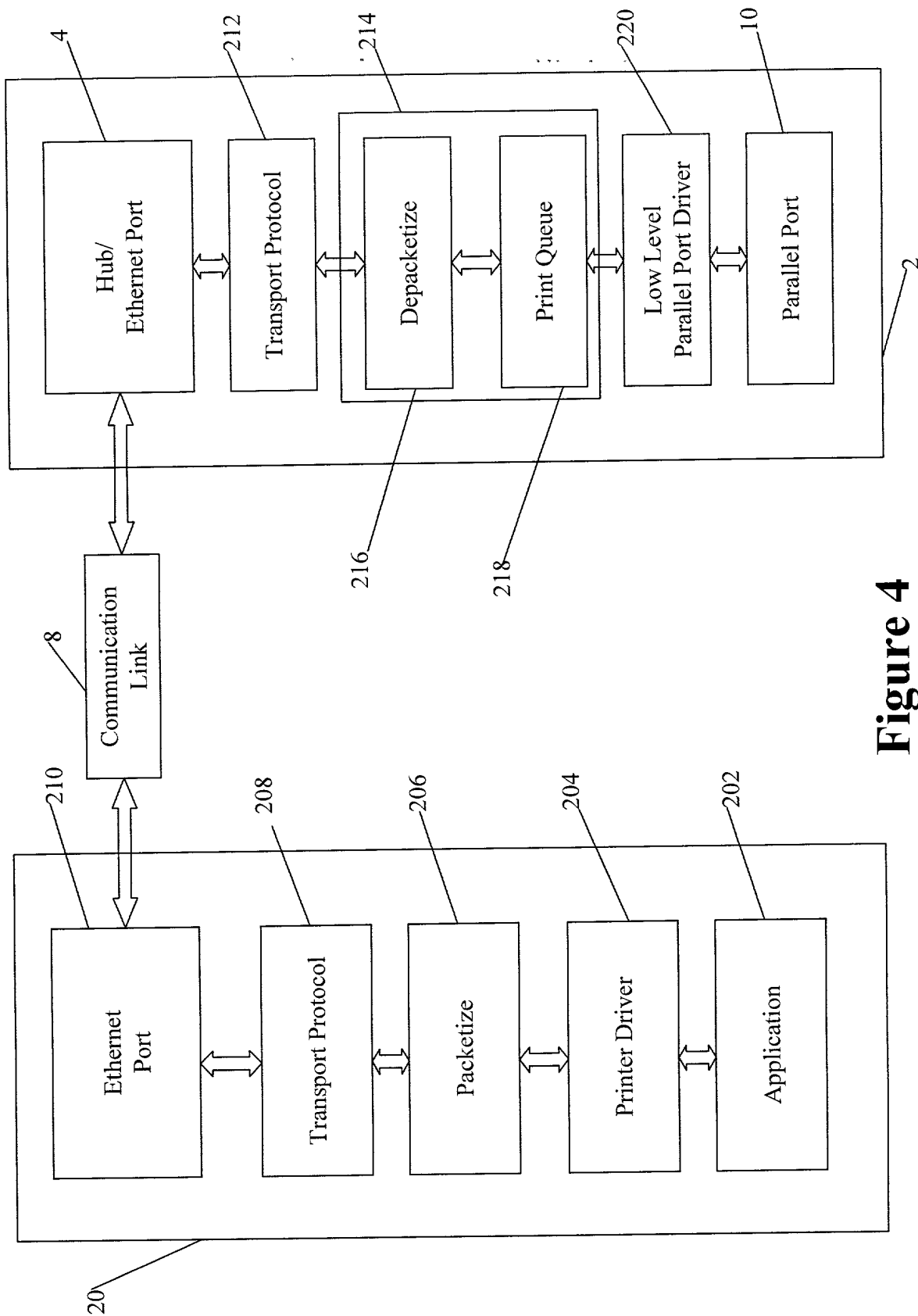


**Figure 3B**



**Figure 3C**

200



**Figure 4**

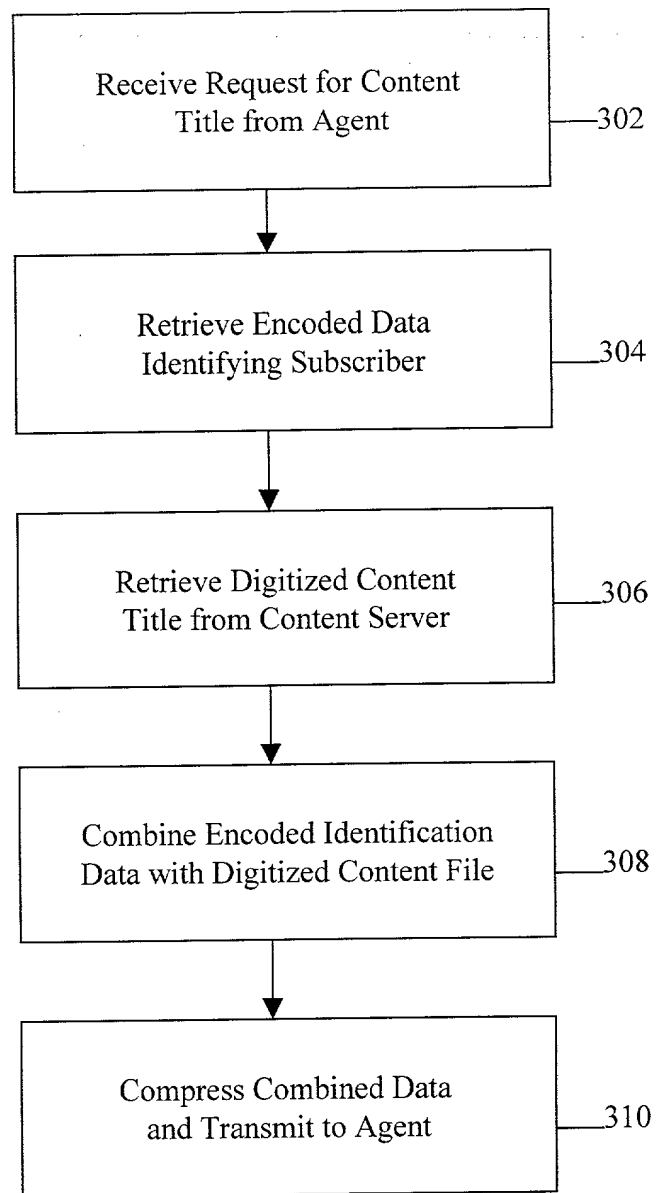


Figure 5

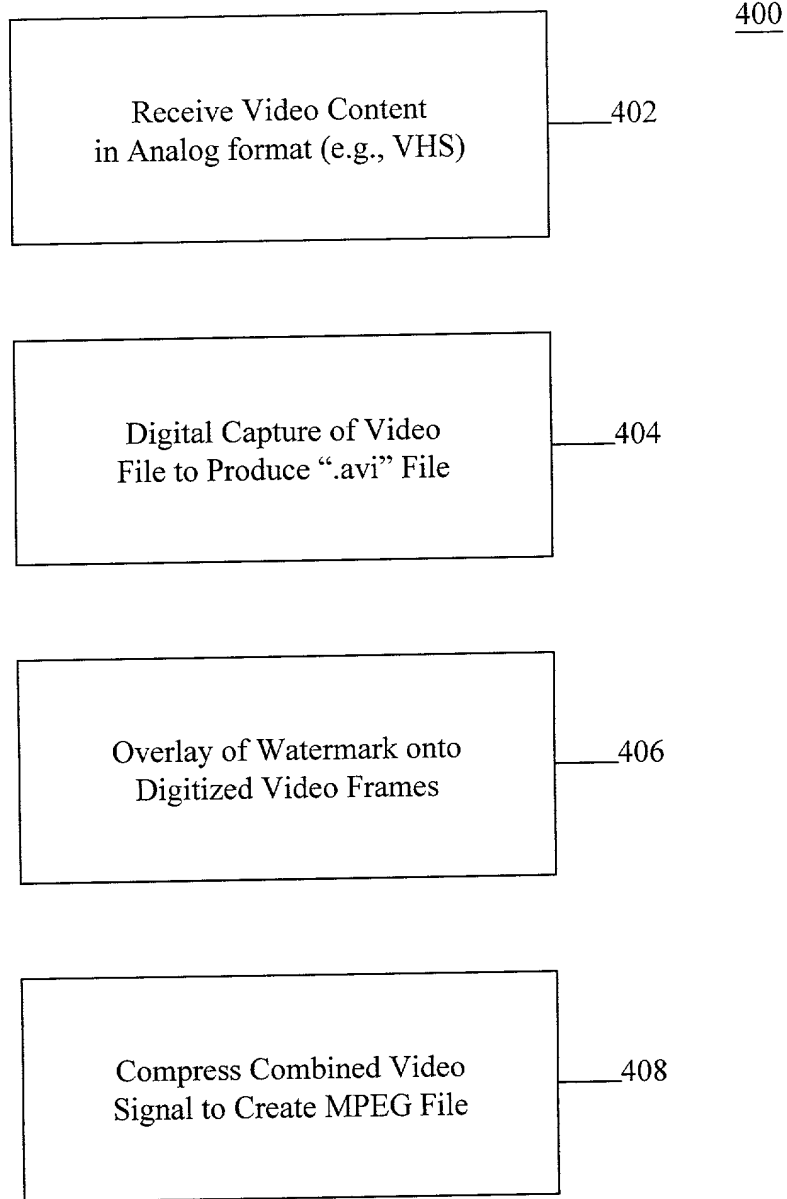


Figure 6



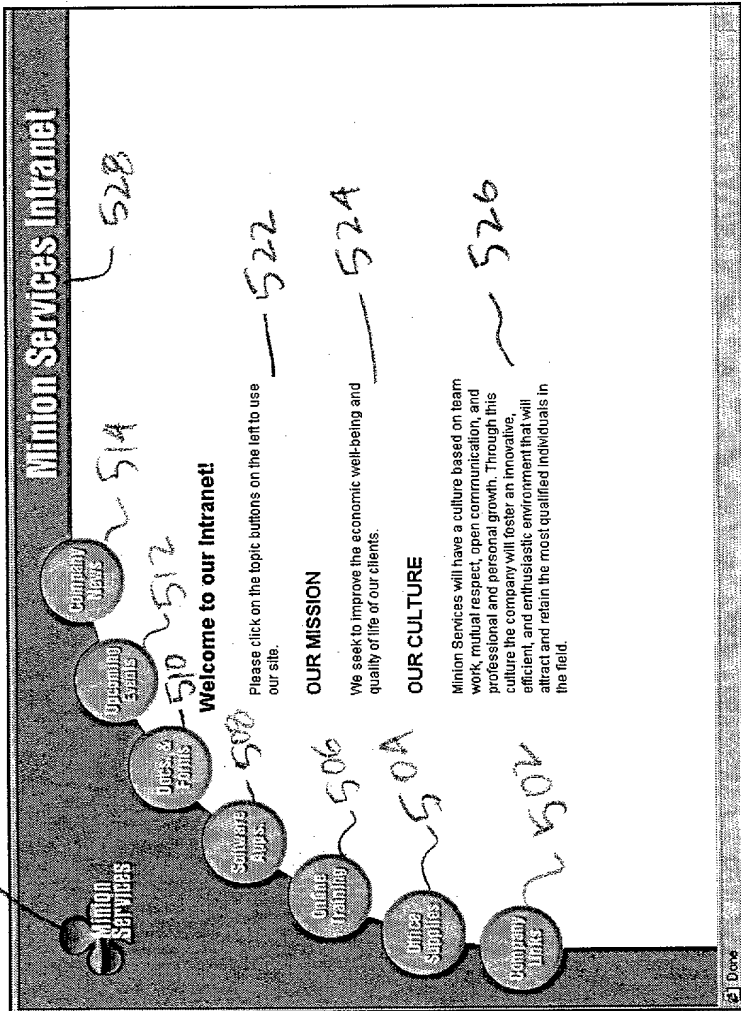


Figure 7

**DECLARATION  
and POWER OF ATTORNEY**

☐ ORIGINAL  
☒ CONTINUATION  
☐ DIVISIONAL

As a below named inventor, I declare that the information given herein is true, that I believe that I am the original, first and sole inventor if only one name is listed at 1 below, or a joint inventor if plural inventors are named below at 1-4, of the invention entitled:

**SYSTEM FOR DELIVERING CONTENT ON-LINE**

Which is described and claimed in:

- ☒ the attached specification or  
☐ the specification in application Serial No. \_\_\_\_\_  
☐ as amended on \_\_\_\_\_

and for which a patent is sought, and that my residence, post office address and citizenship are as stated below next to my name.

I acknowledge my duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations §1.56(a).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

**PRIOR FOREIGN APPLICATION(S)**

COUNTRY	APPLICATION NUMBER	DATE OF FILING Month/Day/Year	PRIORITY CLAIMED UNDER 35 U.S.C. 119
			Yes _____ No _____
			Yes _____ No _____

I hereby claim the benefit under title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below

APPLICATION NO. \_\_\_\_\_ Date \_\_\_\_\_

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

APPLICATION NO.	Filing Date	Status – (patented, pending, abandoned)
09/553,430	April 19, 2000	pending

I hereby appoint

Paul N. Kokulis, Reg. No. 16773; Raymond F. Lippitt, Reg. No. 17519; G. Lloyd Knight, Reg. No. 17698; Carl G. Love, Reg. No. 18781; Kevin E. Joyce, Reg. No. 20508; George M. Sirilla, Reg. No. 18221; Donald J. Bird, Reg. No. 25323; Peter W. Gowdey, Reg. No. 25872; Dale S. Lazar, Reg. No. 28872; Paul E. White, Jr., Reg. No. 32011; Glenn J. Perry, Reg. No. 28458; Kendrew H. Colton, Reg. No. 30368; G. Paul Edgell, Reg. No. 24238; Lynn E. Eccleston, Reg. No. 35861; Timothy J. Klima, Reg. No. 34852; David A. Jakopin, Reg. No. 32995; Mark G. Paulson, Reg. No. 30793; Stephen C. Glazier, Reg. No. 31361; Paul F. McQuade, Reg. No. 31542; Ruth N. Morduch, Reg. No. 31044; Richard H. Zaitlen, Reg. No. 27248; Roger R. Wise, Reg. No. 31204; Jay M. Finkelstein, Reg. No. 21082; Anita M. Kirkpatrick, Reg. No. 32617; Michael R. Dzwonczyk, Reg. No. 36787; W. Patrick Bengtsson, Reg. No. 32456; Jack S. Barufka, Reg. No. 37087; Paul G. Nagy, Reg. No. 37,896; Steven W. Smyrski, Reg. No. 38,312; Eric S. Chen, Reg. No. 43,542; Vivian S. Shin, Reg. No. 43,919; Adam R. Hess, Reg. No. 41835; my patent attorneys of PILLSBURY MADISON & SUTRO LLP, with offices located at 725 South Figueroa Street, Suite 1200, Los Angeles, California, 90017 telephone (213) 488-7100, and

Send correspondence to Mr. Paul G. Nagy, PILLSBURY MADISON & SUTRO LLP, 725 South Figueroa Street, Suite 1200, Los Angeles, California, 90017, and direct telephone calls to Mr. Paul G. Nagy, (213) 488-7584.

1	Full Name of Sole/First Inventor: SHAUN ASTARABADI	
	Residence: LAGUNA NIGUEL CALIFORNIA (City) (State)	Citizenship: USA
	Post Office Address: 27991 Loretha Lane, Laguna Niguel, California 92677	
	Full Name of Sole/Second Inventor: GLENN SWONK	
2	Residence: LAGUNA NIGUEL CALIFORNIA (City) (State)	Citizenship: USA
	Post Office Address: 28552 Murrelet Dr., Laguna Niguel, California 92677	
	Full Name of Sole/Third Inventor: ANDREW McCLOSKEY	
	3	Residence: YORBA LINDA CALIFORNIA (City) (State)
Post Office Address: 5000 Windy Circle, Yorba Linda, California 92887		
Full Name of Sole/Fourth Inventor:		
4		Residence: (City) (State)
	Post Office Address:	

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

SIGNATURE OF INVENTOR 1 <i>Shaun Astarabadi</i>	SIGNATURE OF INVENTOR 2 <i>Glenn Swonk</i>
DATE 8/30/2000	DATE 8/10/2000
SIGNATURE OF INVENTOR 3 <i>Andrew McCloskey</i>	SIGNATURE OF INVENTOR 4
DATE 9/14/2000	DATE